IN THE DRAWING

The attached sheet of drawing includes changes to Fig. 4. This sheet replaces the original sheet including Fig. 4. In Fig. 4, step E15 has been corrected from "Transformation Inverse" to --Inverse Transformation--.

Attachment: Replacement Sheet

REMARKS

Claims 1-26 are presented for examination. Claims 4 and 11 have been amended to define more clearly what Applicant regards as his invention. Claims 1, 4, 8, and 11 are in independent form. Favorable reconsideration is requested.

Applicant notes with appreciation the indication that Claims 2 and 9 would be allowable if rewritten so as not to depend from a rejected claim, and with no change in scope. These claims have not been so rewritten because, for the reasons given below, their base claim is believed to be allowable.

Claims 1, 3, 8, 10, 15, and 17-22 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent 6,442,283 to *Tewfik*. Claims 4, 11, 17, 18, 23, and 26 were rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent 5,613,004 to *Cooperman*. Claims 1, 3, 8, 10, 15, and 17-22 were rejected under 35 U.S.C. § 103(a) as being obvious from *Tewfik* in view of U.S. Patent 5,889,868 to *Moskowitz*; Claims 4-7, 11-14, 17, 18, 23, and 26, as being obvious from U.S. Patent 5,915,027 to *Cox* in view of U.S. Patent 6,104,826 to *Nakagawa*; Claims 16, 24, and 25, as being obvious from *Cox* in view of *Nakagawa*, and further in view of U.S. Patent 6,459,685 to *Mahe*.

Claim 1 is directed to a method of inserting a message into digital data representative of physical quantities, the message including ordered symbols. The method includes the steps of segmenting the data into regions, and associating at least one region with each symbol to be inserted. For each region into which a symbol in question is to be inserted, the method includes the steps of (1) determining a pseudo-random function, from a key which depends on an initial key and on a length of the message, the dependence on

- 14 -

the length of the message being provided either by a dependence on the number of times the symbol has been inserted into other regions or by a dependence on a ranking of the symbol among the ordered symbols, (2) modulating the symbol in question by the previously determined pseudo-random function in order to supply a pseudo-random sequence, and (3) adding the pseudo-random sequence to the region in question.

One notable feature of Claim 1 is determining a pseudo-random function, from a key which depends on an initial key and on a length of the message, the dependence on the length of the message being provided either by a dependence on the number of times the symbol has been inserted into other regions or by a dependence on a ranking of the symbol among the ordered symbols.

Tewfik, as understood by Applicant, relates to a technique for multimedia data embedding in which perceptual weights are computed in order to ensure that the embedded watermark (also called a key in *Tewfik*, see column 1, line 13) is imperceptible.

Applicant notes that *Tewfik* seeks to embed a specific key or watermark, e.g. to prove ownership (see column 1, lines 50-52). In this context, *Tewfik* proposes to use two random keys x1 and x2, one of which is signal dependent (column 5, line 44). This signal dependence is, however, a dependence on the signal into which the watermark is embedded, as is clear from column 5, line 46 of that patent, which states that "x2 is computed from the audio signal" (see also column 5, line 41).

Therefore, nothing in *Tewfik* would teach or suggest determining a pseudo-random function from a key which depends on a length of a message to be inserted, as in Claim 1. In this respect, Applicant notes that the message of Claim 1 includes

ordered symbols (see the second line of claim 1), which are modulated to supply a sequence which is added to the signal, i.e., the message is inserted as a watermark message.

Additionally, Applicant notes that the weighting coefficients W proposed by *Tewfik* can be considered as depending upon an index i, but this index is not representative of the ranking of the symbol being inserted in the message. Again, *Tewfik* fails to take into consideration the length of a message to be embedded and, therefore, cannot teach or suggest the step of determining a pseudo-random function as in Claim 1.

Accordingly, as *Tewfik* discusses the embedding of a specific key or watermark corresponding to a particular bit (see column 5, lines 4-5 of that patent), *Tewfik* is silent as to the use of the length of the message to be inserted in order to determine the pseudo-random function, and, therefore, cannot teach or suggest a dependence on the number of times a symbol has been inserted or on a ranking of the symbol among the ordered symbols, as in Claim 1.

Nothing in *Tewfik* would teach or suggest determining a pseudo-random function, from a key which depends on an initial key and on a length of the message, the dependence on the length of the message being provided either by a dependence on the number of times the symbol has been inserted into other regions or by a dependence on a ranking of the symbol among the ordered symbols, as recited in Claim 1.

Accordingly, Claim 1 is seen to be patentable over *Tewfik*.

Independent Claim 8 recites features similar in many relevant respects to those discussed above with respect to Claim 1 and therefore is also believed to be patentable over *Tewfik* for at least the reasons discussed above.

Furthermore, even if the combination of *Tewfik* and *Moskowitz* were permissible, the hypothetical combination would not include the determining step of Claim 1, as neither *Tewfik* nor *Moskowitz* would teach or suggest the recited dependence on the length of the message as in Claim 1. *Moskowitz* would not supply what is missing from *Tewfik*.

That is, nothing in *Tewfik* and *Moskowitz*, whether considered either separately or in any permissible combination (if any) would teach or suggest determining a pseudo-random function, from a key which depends on an initial key and on a length of the message, the dependence on the length of the message being provided either by a dependence on the number of times the symbol has been inserted into other regions or by a dependence on a ranking of the symbol among the ordered symbols, as recited in Claim 1.

Accordingly, Claim 1 is seen to be patentable over *Tewfik* and *Moskowitz*, whether considered either separately or in any permissible combination (if any).

Independent Claim 8 recites features similar in many relevant respects to those discussed above with respect to Claim 1 and therefore is also believed to be patentable over *Tewfik* and *Moskowitz* for at least the reasons discussed above.

Claim 4 is directed to a method for extracting a message from digital data representative of physical quantities, the message including ordered symbols. The method includes the steps of (1) segmenting the data into regions, (2) extracting a length of an inserted message, from a set of length values, based on the digital data, and (3) extracting the inserted message. The extracting step includes a step of generating a key which

depends on an initial key and on an assumed length for the inserted message from the set of length values (see, e.g., the present specification at page 12, lines 18-20).

One notable feature of Claim 4 is an extracting step which includes generating a key which depends on an initial key and on an assumed length for the inserted message from the set of length values (see, e.g., the present specification at page 12, lines 18-20.)[1]

Cooperman, as understood by Applicant, relates to a watermarking method in which masks are used for synchronization purposes. At the decoder's end, a number of bits is derived due to these masks and compared to bits at the start of a message delimiter (see column 12, lines 43-46).

Nothing in *Cooperman* would teach or suggest using an assumed length for an inserted message, taken among a set of possible length values, in order to generate a specific key, depending on this assumed length, as in Claim 4. By virtue of the features of Claim 4, a correlation can be calculated that is indicative of whether the assumed length is the length of the inserted message (see, e.g., the present specification from page 12, line 17, to page 13, line 13).

Applicant has found nothing in *Cooperman* that would teach or suggest an extracting step which includes generating a key which depends on an initial key and on an assumed length for the inserted message from the set of length values, as recited in Claim 4.

---

[1]/It is of course to be understood that the references to various portions of the present application are by way of illustration and example only, and that the claims are not limited by the details shown in the portions referred to.

Accordingly, Claim 4 is seen to be patentable over *Cooperman.*

Independent Claim 11 recites features similar in many relevant respects to those discussed above with respect to Claim 4 and therefore is also believed to be patentable over *Cooperman* for at least the reasons discussed above.

The general nature of *Cox* and *Nakagawa* has been discussed adequately in previous papers, and it is not believed to be necessary to repeat that discussion. Nothing has been found in *Cox* and *Nakagawa*, whether considered either separately or in any permissible combination (if any) that would teach or suggest an extracting step which includes generating a key which depends on an initial key and on an assumed length for the inserted message from the set of length values, as recited in Claim 4.

Accordingly, Claim 4 is seen to be patentable over *Cox* and *Nakagawa*, whether considered either separately or in any permissible combination (if any).

Independent Claim 11 recites features similar in many relevant respects to those discussed above with respect to Claim 4 and therefore is also believed to be patentable over *Cox* and *Nakagawa* for at least the reasons discussed above.

A review of the other art of record has failed to reveal anything which, in Applicant's opinion, would remedy the deficiencies of the art discussed above, as references against the independent claims herein. Those claims are therefore believed patentable over the art of record.

The other claims in this application are each dependent from one or another of the independent claims discussed above and are therefore believed patentable for the same reasons. Since each dependent claim is also deemed to define an additional aspect of

the invention, however, the individual reconsideration of the patentability of each on its own merits is respectfully requested.

In view of the foregoing amendments and remarks, Applicant respectfully requests favorable reconsideration and early passage to issue of the present application.

Applicant's undersigned attorney may be reached in our New York office by telephone at (212) 218-2100. All correspondence should continue to be directed to our below listed address.

Respectfully submitted,

Raymond A. DiPerna
Attorney for Applicant
Registration No.: 44,063

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200